N1 medium

Jack, DarkCrystal

Titolo nota 04/09/2018

- Somme di 2 e 4 quadrati
- Problema del cerchio di Gauss
- Ciclotomia, φ, esistenza $g : \langle g \rangle = G$
- $\left(\frac{\cdot}{p}\right)$ e casi elementari di $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$

Cauchy-Schwarz $\quad (a^2+b^2)(c^2+d^2) \geq (ac+bd)^2$

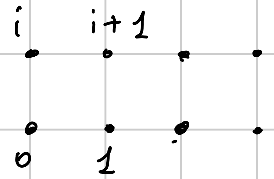
Id. Lagrange $\quad (a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$

$\mathbb{Z}[i]$ anello degli interi di Gauss

$N(a+bi) = (a+bi)(a-bi) = a^2+b^2 \qquad a+bi = z$

$N(z) = z \cdot \bar{z}$

$\mathbb{Z}[i] = \{(a+bi) : a, b \in \mathbb{Z}\}$



$z = a+bi \qquad w = c-di \qquad N(z \cdot w) = N(z) \cdot N(w)$

$z \cdot w = (ac+bd) - i(ad-bc)$

Id. Lagrange in più variabili

$$\sum_{k=1}^{n} a_k^2 \cdot \sum_{k=1}^{n} b_k^2 = \underbrace{\left(\sum_{k=1}^{n} a_k b_k\right)^2}_{\langle \cdot,\cdot \rangle^2} + \overbrace{\underbrace{\sum_{1 \leq j < k \leq n} (a_j b_k - a_k b_j)^2}_{|v \times w|^2}}^{CS \iff \geq 0}$$

$A = \{\square + \square\}$ è un semigruppo : $a \in A,\ b \in A \longrightarrow ab \in A$

Quali interi si scrivono come a^2+b^2?

- se $n \equiv 3\ (4)$, $n \notin \{\square + \square\}$ $\qquad m^2 \pmod 4 \in \{0,1\}$
- $n = 21 = 0^2 + \sqrt{21}^2$

$$1^2 + \sqrt{20}^2$$
$$2^2 + \sqrt{17}^2$$
$$3^2 + \sqrt{12}^2$$

Quali primi si scrivono come a^2+b^2?
di certo non quelli della forma $4k+3$,
2 sì, $2 = 1^2+1^2$ e

(Conj) $\forall p \equiv 1\ (4)\ \exists a,b : p = a^2+b^2$

[(Atto di fede) $\forall p \equiv 1\ (4)$ -1 è residuo quadratico $\pmod p$,
ossia $\exists m \in \mathbb{Z} : m^2+1 \equiv 0 \pmod p$]

Metodo di discesa di Fermat
$p = 101 = 10^2+1^2$

$$a^2+b^2 = kp \iff a^2+b^2 \equiv 0 \pmod p$$

$0 < a,b < \frac{p}{2}$ $\qquad \underline{k < \frac{p}{2}}$

$$\Updownarrow$$

$$(ab^{-1})^2 + 1 \equiv 0 \pmod p$$ atto di fede

$$x^2 \equiv (-x)^2 \bmod p$$

riduciamo a e b $\pmod k$ ottenendo a_1 e b_1

$a_1^2 + b_1^2 = kq$

$$\underbrace{(aa_1 + bb_1)}_{\equiv 0\ (k)}{}^2 + \underbrace{(ab_1 - ba_1)}_{\equiv 0\ (k)}{}^2 = k^2 pq$$

$$\left(\frac{aa_1+bb_1}{k}\right)^2 + \left(\frac{ab_1-ba_1}{k}\right)^2 = pq \qquad q < k$$

reiterando l'argomento, $p \in A$.

$p \equiv 1\ (4) \longrightarrow p = a^2 + b^2$ rappresentazione "unica"

a meno di $a \leftrightarrow b$

$a \leftrightarrow -a$

$b \leftrightarrow -b$

Se tutti i primi $p \mid n$ sono della forma $4k+1$,

$n \in A$

$$r_2(n) = \left|\left\{ (a,b) \in \mathbb{Z}^2 : a^2 + b^2 = n \right\}\right|$$

$$r_2(n) = 4 \cdot \underset{\tau(n)}{d(n)}$$

$25 = 5 \cdot 5$ $\quad 5 = 1^2 + 2^2$ $\quad 5 = 1^2 + 2^2$

$25 =$
$0^2 + 5^2$
$5^2 + 0^2$
$3^2 + 4^2$ $\quad (-3)^2 + 4^2$ $\quad - - \quad + -$
$4^2 + 3^2$ $\quad (-4)^2 + (3)^2$ $\quad - - \quad + -$
$0^2 + (-5)^2$
$(-5)^2 + 0^2$

Se $p \equiv 3\ (4)$ divide n con molteplicità dispari

$\nu_p(n) \equiv 1\ (2)$

$\nu_p(n) = \max\{ m \in \mathbb{N} : p^m \mid n \}$

allora $n \notin A$

Se $p \equiv 3\ (4)$ divide n con molteplicità pari

e tutti gli altri divisori primi di n

sono $\equiv 1\ (4)$, allora $n \in A$

$\forall\ n = a^2 + b^2, \quad a, b \equiv 0 \pmod p$

$n \in A \longrightarrow 2n \in A$ $\qquad \underset{n \equiv 0\ (2)}{n \in A} \longrightarrow \frac{n}{2} \in A$

$$(a-b)^2 + (a+b)^2 = 2(a^2 + b^2)$$

Gli elementi di A sono tutti e soli gli interi per cui $p \equiv 3\,(4),\ p \mid n \longrightarrow \nu_p(n) \equiv 0\,(2)$

$$r_2(n) = 4(\chi_4 * 1)(n) = 4 \sum_{d \mid n} \chi_4(d)$$

convoluzione di Dirichlet

$$\chi_4(m) \begin{cases} 1 & m \equiv 1\,(4) \\ -1 & m \equiv -1\,(4) \\ 0 & m \text{ pari} \end{cases}$$

$r_2(n)$ è un multiplo di una funzione moltiplicativa.

$\mathbb{Z}[i]$ è euclideo $\longrightarrow$ $\mathbb{Z}[i]$ è UFD

$$n = (a+bi)(a-bi)$$

---

in $\mathbb{Z}[i]$ i primi sono i primi di $\mathbb{Z}$ della forma $4k+3$ e gli elementi $\pm a \pm bi$ dove $a^2+b^2 = p \equiv 1\,(4)$

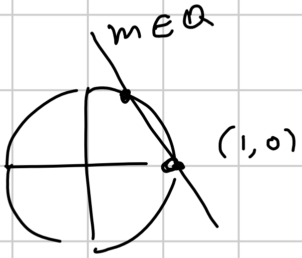
$1, -1, i, -i$

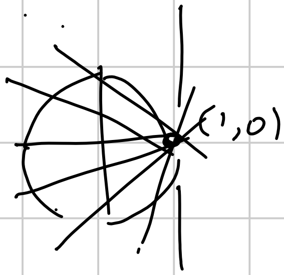
$B = \{ \square + 2 \cdot \square \}$ investigazione lasciata al lettore.

Formule parametriche $\longleftrightarrow$ Struttura delle terne pitagoriche primitive

$a^2+b^2 = c^2 \quad \gcd(a,b) = 1$

$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$





$$\begin{cases} y = m(x-1) \\ x^2+y^2 = 1 \end{cases} \qquad m \in \mathbb{Q}$$

$x^2 + m^2(x-1)^2 = 1$

$x = 1$ è sicuramente sol di

$\forall (x,y) \in S^1$ $\quad \underbrace{x = \frac{1-t^2}{1+t^2} \quad y = \frac{2t}{1+t^2}}$ per $t \in \mathbb{Q}$

$\uparrow$

$\mathbb{Q}^2$

caso $n=4$

FLT

se $a^2+b^2=c^2$ e $\gcd(a,b)=1$ allora

$a = 2pq \quad b = p^2-q^2 \quad c = p^2+q^2$

$\gcd(p,q)=1$, $p+q \equiv 1\ (2)$

$$\bar{d}(A) = \limsup_{n\to+\infty} \frac{|[1,n]\cap A|}{n}$$

$$|A \cap [1,n]| \leq \frac{C_0\, n}{\sqrt{\log n}}$$

$A \quad A$ densità 0

$A+A$ densità 1

$B = \{\square+\square+\square+\square\}$

OSS. 1 è un semigruppo per la norma su $\mathbb{H}$

$\mathbb{C} = \mathbb{R}[x]/(x^2+1)$

1

$a+bi+cj+dk$

$(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) = \square+\square+\square+\square$

$B = \mathbb{N}$ $\qquad r_4(n) = |\{(a,b,c,d) \in \mathbb{Z}^4 : a^2+b^2+c^2+d^2 = n\}|$

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ d \not\equiv 0\,(4)}} d$$

$\exists\, u, v : \quad u^2+v^2 \equiv -1 \ (p)$ (Chevalley)

$$(a+ib) - (c+id)(u+iv)$$

con $a^2+b^2+c^2+d^2 \leq R^2$

$$a = a_1 - a_2 \qquad b = b_1 - b_2$$

Teorema di Minkowski per i corpi convessi e simmetrici.

Prodotto triplo di Jacobi $\xrightarrow[0]{\partial/\partial x}$ serie di Lambert

$$\underset{\Theta(z)}{\underset{\parallel}{\sum_{n\in\mathbb{Z}} z^{n^2}}} = \prod_{m\geq 1} (\quad)(\quad)(\quad)$$

$$r_2(n) = [z^n]\,\Theta(z)^2 \qquad r_4(n) = [z^n]\,\Theta(z)^4$$

Serie di Lambert

$$\sum_{m\geq 1} \frac{x^m}{1-x^m} = \sum_{m\geq 1}\sum_{k\geq 1} x^{mk} = \sum_{n\geq 1} x^n\, d(n)$$

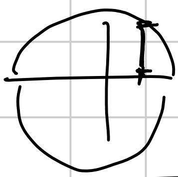
$$\sum_{n\geq 0} \frac{(-1)^n\, d(2n+1)}{2n+1} = \frac{\pi^2}{16}$$ Esercizio

Hint: cos'è $\chi_4 * \chi_4(n) = \sum_{d\mid n} \chi_4(d)\,\chi_4\left(\frac{n}{d}\right)$?

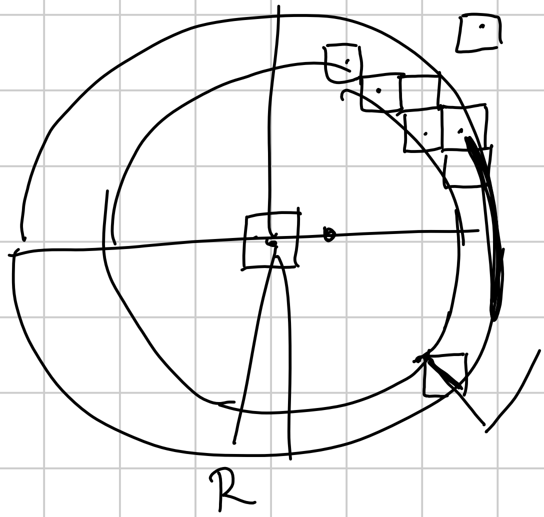
Cosa ci dice l'algebra delle serie di Dirichlet ?

Quanti elementi di $\mathbb{Z}\times\mathbb{Z}$ soddisfano $x^2+y^2 \leq R^2$?

$$2\sum_{z=-R}^{R} \left\lfloor \sqrt{R^2-z^2} \right\rfloor + 2R-1$$



$$1 + \sum_{m=1}^{R^2} r_2(m)$$



$$\pi(R-\sqrt{2})^2 \leq \ldots \leq \pi(R+\sqrt{2})^2$$

$$\pi R^2 + E(r)$$

$$|E(r)| \leq k \cdot r$$

Teorema del cerchio di Gauss

l'ordine medio di r_2 è π

Voronoi $\quad \pi R^2 + E(r)$

$$|E(r)| \leq k \cdot r^{2/3}$$

Stime delle f. di Bessel

$$\lim_{x \to 1^-} \sqrt{1-x} \sum_{n=0}^{+\infty} x^{n^2} = \frac{\sqrt{\pi}}{2}$$

$$\frac{\theta(x)-1}{2} \sim \frac{1}{2}\sqrt{\frac{\pi}{1-x}} \quad \text{per } x \to 1^-$$

formule di sommazione di Poisson

$$\left(\sum_{n\geq 0} x^{n^k}\right)^k \sim \frac{\Gamma\left(1+\frac{1}{k}\right)^k}{1-x} \quad \text{per } x \to 1^-$$

(Hardy 192x)

Ciclotomici: $\Phi_n(x)$ è il poly. min. su $\mathbb{Q}$ di $\exp\left(\frac{2\pi i}{n}\right)$

$\Phi_n(x)$ è monico e a coeff. interi.

$\deg \Phi_n = \varphi(n)$

φ è moltiplicativa e $\varphi(p^k) = (p-1)p^{k-1}$

$\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^*|$ $\qquad \left.\begin{array}{c}\mathbb{Z}/n\mathbb{Z}^* \times \mathbb{Z}/m\mathbb{Z}^* \simeq \mathbb{Z}/nm\mathbb{Z}^* \\ \gcd(n,m)=1\end{array}\right\}$ TC R

$\varphi(n) \cdot \varphi(m) = \varphi(nm)$

$|\mathbb{Z}/p^k\mathbb{Z}^*| = p^k - p^{k-1} = p^{k-1}(p-1)$

$\mathbb{Z}/p\mathbb{Z}^*$ è ciclico, ossia $\exists g \in \mathbb{Z}/p\mathbb{Z}^* : \langle g \rangle = \mathbb{Z}/p\mathbb{Z}^*$

$p=7 \quad \mathbb{Z}/7\mathbb{Z}^* = \{\overset{NO}{1}, \overset{NO}{2}, 3, \overset{NO}{4}, 5, \overset{NO}{6}\}$ $\qquad |\langle g \rangle| = o(g)$

$\langle 1 \rangle = \{1\}$ $\qquad$ è un divisore di $|G|$

$\langle 2 \rangle = \{1, 2, 4\}$

$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\}$

$\langle 4 \rangle = \{1, 4, 2\}$ $\qquad \langle 5 \rangle = \{1, 5, 4, 6, 3, 2\}$

$\langle g \rangle = G \iff \langle g^{-1} \rangle = G$

se $|G|$ è pari e $h = g^2$ allora $\langle h \rangle \neq G$

Preso $m = p-1 = |\mathbb{Z}/p\mathbb{Z}^*| = q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k}$

$g \in \mathbb{Z}/p\mathbb{Z}^*$ è generatore se e solo se

$$g^{\frac{p-1}{q_j}} \not\equiv 1 \pmod p \quad \forall j \in [1, k]$$

In $\mathbb{Z}/p\mathbb{Z}^*$ ci sono $\varphi(\varphi(p)) = \varphi(p-1)$ generatori

$(\mathbb{Z}/p\mathbb{Z}, +)$ $(\mathbb{Z}/p\mathbb{Z}^*, \cdot)$ $\mathbb{F}_p$ campo finito con p elementi

$x^m - 1$ ha $\leq m$ radici in $\mathbb{F}_p$

$x^2 - 1$ ha ≤ 2 radici in $\mathbb{F}_p$

$x^3 - 1$ ha ≤ 3 radici in $\mathbb{F}_p$

$x^{p-1} - 1$ = prodotto di poly ciclotomici

$\deg \Phi_m = \varphi(m)$

$\varphi * 1 = \mathrm{Id}$ $\qquad \underbrace{\sum_{d|n} \varphi(d)}_{\text{f. molt.}} = n$

$$\sum_{d|p^k} \varphi(d) = \sum_{j=0}^{k} \varphi(p^j) = 1 + \underbrace{\sum_{j=1}^{k} (p-1)p^{j-1}}_{\text{telescopica}} = p^k$$

$\mathbb{Z}/p\mathbb{Z}^*$ c'è un generatore $\longrightarrow$ $\mathbb{Z}/p^k\mathbb{Z}^*$ c'è un generatore

p dispari

$\mathbb{Z}/2\mathbb{Z}^*$ $\quad \mathbb{Z}/4\mathbb{Z}^*$

$\mathbb{Z}/2^m\mathbb{Z}^*$ $\overset{m \geq 3}{=} \{\pm 5^a\}$

Sollevamento henseliano.

---

www.matemate.it $\rightarrow$ Appunti

$\downarrow$

Taranto

- dispense Jack
- dispense Pete Clark

COMPLEMENTI SUI RESIDUI QUADRATICI

Simbolo di Legendre modulo p primo

n e' residuo quadratico mod p

$\iff x^2 \equiv n \mod p$ si risolve

Def $$\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{se } n \text{ e' R.Q. mod } p \\ -1 & \text{se non lo e'} \\ 0 & \text{se } p \mid n \end{cases}$$

$$\#\{\text{quadrati} \neq 0 \ (p)\} = \frac{p-1}{2}$$

$$x \longmapsto x^2$$

e' 2 - a - 1 da $(\mathbb{Z}/_p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/_p\mathbb{Z})^*$

$$p-1 \longmapsto \frac{p-1}{2}$$

Criterio di Eulero

$$\left(\frac{n}{p}\right) = +1 \iff n^{\frac{p-1}{2}} \equiv 1 \mod p$$

$$\left(\frac{n}{p}\right) \equiv \underbrace{n^{\frac{p-1}{2}}}_{} \pmod p$$

sempre ± 1 : il suo quadrato e' $n^{p-1} \equiv 1 \pmod p$

Se n è un quadrato, $n \equiv a^2 \mod p$,

$$n^{\frac{p-1}{2}} \equiv (a^2)^{\frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \ (p)$$

L'equazione $X^{\frac{p-1}{2}} \equiv 1 \mod p$

ha $\leq \frac{p-1}{2}$ soluzioni (grado)

$\geq \frac{p-1}{2}$ soluzioni ($\square$)

Se prendo n non RQ, $n^{\frac{p-1}{2}}$ non

può fare 1 (altrimenti avrei

$> \frac{p-1}{2}$ soluzioni di $X^{\frac{p-1}{2}} \equiv 1$),

e quindi è $\equiv -1 \pmod p$

Cor -1 è RQ mod $p \iff p \equiv 1 \ (4)$

(o $p = 2$)

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & p \equiv 1 \ (4) \\ -1 & p \equiv 3 \ (4) \end{cases}$$

Cor. 2 $$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$(ab)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}}(b)^{\frac{p-1}{2}} \mod p$$

Conseguenza $(x^2-2)(x^2-3)(x^2-6) \equiv 0\ (p)$

ha soluzione $\forall p$

Se $\left(\frac{2}{p}\right)=+1$ OK

Se $\left(\frac{3}{p}\right)=+1$ OK

Altrimenti $\left(\frac{2}{p}\right)=\left(\frac{3}{p}\right)=-1$, e quindi

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=(-1)(-1)=+1$$

Simile x^4+1 si fattorizza modulo ogni primo

è riducibile

Reciprocità quadratica

$$\left(\frac{28}{32003}\right) = \left(\frac{2}{32003}\right)\left(\frac{14}{32003}\right).$$

$$= \left(\frac{2}{32003}\right)^2 \left(\frac{7}{32003}\right)$$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \qquad p, q \text{ dispari}$$

$$= \begin{cases} \left(\frac{q}{p}\right) & \text{se } p \equiv 1\ (4) \text{ o } q \equiv 1\ (4) \\ -\left(\frac{q}{p}\right) & \text{se } p \equiv q \equiv 3\ (4) \end{cases}$$

Es $\quad \left(\frac{7}{32003}\right) = -1 \cdot \left(\frac{32003}{7}\right)$

$$= (-1) \cdot \left(\frac{-1}{7}\right) = +1$$

E $p = 2$? $\quad \left(\frac{2}{p}\right) = +1 \iff p \equiv \pm 1\ (8)$

Caso speciale

$$\left(\frac{-3}{p}\right) = +1 \iff \left(\frac{p}{3}\right) = +1$$

$$\Updownarrow$$

$$p \equiv 1 \ (3)$$

L'equazione $x^3 \equiv 1 \pmod p$ ha

$$\begin{cases} 1 \quad \text{soluzione} \quad \text{se } p \equiv 2 \ (3) & (1) \\ 3 \quad \text{soluzioni} \quad \text{se } p \equiv 1 \ (3) & (2) \end{cases}$$

(1) $x^3 \equiv 1 \ (p)$ $\qquad \mathrm{ord}_p(x) = 1 \ \cancel{\text{o } 3}$

$\mathrm{ord}_p(x) \mid p-1$

(2) Le tre soluzioni sono $x \equiv 1$, $x \equiv g^{\frac{p-1}{3}}$, $x \equiv g^{\frac{p-1}{3} \cdot 2}$ con g generatore

$$x^3 - 1 = (x-1)\underbrace{(x^2+x+1)}_{\text{0 o 2 radici}}$$

$p \equiv 2$ o $p \equiv 1 \ (3)$

$$x \equiv \frac{-1 \pm \sqrt{-3}}{2} \pmod p.$$

$x^2 + x + 1 \equiv 0 \mod p$ ha delle soluzioni.

$$\iff \left(\frac{-3}{p}\right) = +1 \quad \iff \quad p \equiv 1 \ (3).$$

$$\left(\frac{2}{p}\right) \qquad (1+i)^2 = 2i$$

$$\Rightarrow 2 = \frac{(1+i)^2}{i}$$

$$\left(\frac{2}{p}\right) \equiv \left(\frac{(1+i)^2}{i}\right)^{\frac{p-1}{2}} \equiv \frac{(1+i)^{p-1}}{i^{\frac{p-1}{2}}}$$

$$\equiv \frac{(1+i)^p}{(1+i)\, i^{\frac{p-1}{2}}} \equiv \frac{1+i^p}{(1+i)\, i^{\frac{p-1}{2}}} \pmod p.$$

ESERCIZI

① Contare il numero di soluzioni di

$$X^2 + Y^2 \equiv 1 \pmod p$$

Supponiamo $p \equiv 1 \bmod 4$ e sia (con notazione ovvia) $i \in \mathbb{Z}$ t.c. $i^2 \equiv -1 \ (p)$

$$(X+iy)(X-iy) \equiv 1 \bmod p$$

L'eqz $\quad u \cdot v \equiv 1 \bmod p$

ha $p-1$ soluzioni; quella sopra anche: $\begin{cases} X + iy = u \\ X - iy = v \end{cases} \quad \begin{cases} X = \frac{u+v}{2} \\ y = \frac{u-v}{2i} \end{cases}$

Supponiamo invece $p \equiv 3 \bmod 4$.

$$X^2 + Y^2 \equiv 1 \pmod p$$

$Y \equiv 0 \longrightarrow 2$ soluzioni

$Y \not\equiv 0 \ (p) \qquad \left(\frac{X}{Y}\right)^2 + 1 \equiv \left(\frac{1}{Y}\right)^2 \bmod p$

$$1 \equiv \left(\frac{1}{y}\right)^2 - \left(\frac{x}{y}\right)^2 \mod p$$

$$\equiv u^2 - v^2 \equiv (u+v)(u-v)$$

$$\equiv A \cdot B \ (p)$$

$p-1$ soluzioni

CONCLUSIONE : se $p \equiv 3 \ (4)$ ci sono $p+1$ soluz.

soluzioni di $x^2 \equiv n \mod p$ e'

$$1 + \left(\frac{n}{p}\right)$$

Soluz di $x^2 + y^2 \equiv 1 \ (\mod p)$

$$= \sum_{x=0}^{p-1} \left(\# \text{ soluz di } y^2 \equiv 1 - x^2 \ (p) \right)$$

$$= \sum_{x=0}^{p-1} \left(1 + \left(\frac{1-x^2}{p} \right) \right)$$

$$\equiv \sum_{x=0}^{p-1} \left(1 + (1-x^2)^{\frac{p-1}{2}} \right) \mod p$$

$$\equiv \sum_{x=0}^{p-1} \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} (-x^2)^j \mod p$$

PARENTESI: SOMME DI POLINOMI MOD p

$$\sum_{x=0}^{p-1} x \equiv 0 \quad (p) \qquad p>2$$

$$\sum_{x=0}^{p-1} x^2 \equiv \frac{(p-1)p(2p-1)}{6} \equiv 0 \, (p) \qquad p>3$$

$$\sum_{x=0}^{p-1} x^{p-1} \equiv -1 \quad (p)$$

$\boxed{\text{LEMMA IMPORTANTE}}$ Sia $f(x)$ un polinomio di grado d. Se $p-1>d$, allora

$$\sum_{x=0}^{p-1} f(x) \equiv 0 \pmod p$$

$\boxed{\text{DIM}}$ Basta farlo per i monomi, $f(x) = a \cdot x^d$, anzi, $f(x) = x^d$

$$\sum_{x=0}^{p-1} x^d \underset{d>0}{\equiv} \sum_{x=1}^{p-1} x^d$$

$$\equiv \sum_{k=0}^{p-2} (g^k)^d$$

$d<p-1$

$(p-1 \nmid d)$

$$\equiv \frac{(g^d)^{p-1} - 1}{g^d - 1} \equiv 0 \ (p)$$

$\square$

$$\equiv \sum_{x=0}^{p-1} \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} (-x^2)^j \mod p$$

$$\equiv \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} \underbrace{\left(\sum_{x=0}^{p-1} (-x^2)^j \right)}$$

di grado $< p-1$

tranne che per $j = \frac{p-1}{2}$

$$\equiv \binom{(p-1)/2}{(p-1)/2} \cdot (-1)^{\frac{p-1}{2}} \sum_{x=0}^{p-1} x^{p-1}$$

$$\equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \pmod p$$

$\# \text{ Soluzioni}$ $\begin{cases} \equiv -(-1)^{\frac{p-1}{2}} \ (p) \\ 0 < \cdot < 2p \end{cases}$

$\# \text{ Soluz} : \cancel{1}, p-1, p+1, \cancel{2p-1}$

$\#$ Soluz è pari: se c'è (x,y) c'è $(-x,-y)$

$$\# \text{ soluz} = p - \left(\frac{-1}{p}\right)$$

Cor (del conto) $\#$ Soluz di

$$x^2 + y^2 \equiv a \pmod p$$

è sempre $p - \left(\frac{-1}{p}\right)$ (se $a \neq 0$)

IMO SL 2010 N3

Trovare il minimo n per cui esistono polinomi a coefficienti razionali

$$f_1(x), \dots, f_n(x) \quad \text{t.c.}$$

$$f_1(x)^2 + \dots + f_n(x)^2 = x^2+7$$

$\boxed{n=8}$ $f_1(x) = x, \quad f_i(x) = 1 \quad i = 2, \dots, 8$

$\boxed{n=5}$ $(x)^2 + (2)^2 + (1)^2 + (1)^2 + (1)^2$

$\deg f_i(x) \leq 1$

$f_i(x) = a_i x + b_i \qquad a_i, b_i \in \mathbb{Q}$

$$(a_1 x + b_1)^2 + \dots + (a_4 x + b_4)^2 = x^2 + 7$$

$$\begin{cases} a_1^2 + a_2^2 + a_3^2 + a_4^2 = 1 & \|a\|^2 = 1 \\ a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4 = 0 & a \perp b \\ b_1^2 + \dots + b_4^2 = 7 & \|b\|^2 = 7 \end{cases}$$

MIRACOLO

$$7 = (a_1^2 + \dots + a_4^2)(b_1^2 + \dots + b_4^2) =$$

$$= (a_1 b_1 + a_2 b_2 + \dots + a_4 b_4)^2 + (\quad)^2 + (\quad)^2 + (\quad)^2$$

$$= \frac{A^2}{D^2} + \frac{B^2}{D^2} + \frac{C^2}{D^2} \qquad A, B, C, D \text{ interi}$$

$A^2 + B^2 + C^2 = 7D^2$: la guardo mod 8.

Se D e' dispari trovo $A^2 + B^2 + C^2 \equiv 7 \ (8)$, che non si risolve. Quindi D e' pari.

$\Rightarrow A^2 + B^2 + C^2 \equiv 0 \mod 4$

$\Rightarrow A, B, C$ tutti pari

Per discesa infinita non ci sono soluzioni (tranne $A = B = C = D = 0$, che pero' non da' soluzioni del problema iniziale)

Esercizio

Determinare tutti i K interi positivi tali che

$$K+1 \mid 2^{k}+1$$

$2^{k}+1$ è dispari! Quindi k è pari

$K = 2k_1 \qquad 2K_1+1 \mid 2^{2k_1}+1$

Tutti i fattori primi di $2^{2k_1}+1$ sono $\equiv 1 \ (4)$:

se $p \equiv 3 \ (4)$ dividesse $2^{2k_1}+1$, si avrebbe

$$-1 \equiv \left(2^{k_1}\right)^2 \mod p, \text{ assurdo}$$

Quindi $2k_1+1 \equiv 1 \ (4) \Rightarrow k_1 = 2k_2$

$$4K_2+1 \mid 2^{4K_2}+1$$

Sia p un divisore primo di $2^{4k_2}+1$.

$$2^{4k_2} \equiv -1 \ (p) \Rightarrow 2^{8k_2} \equiv 1 \ (p)$$

$$\mathrm{ord}_p(2) \mid p-1$$

$$\mathrm{ord}_p(2) \mid 8K_2 \qquad \mathrm{ord}_p(2) \nmid 4K_2$$

q^h : se $q \neq 2$ ok per entrambe

$$\Rightarrow \quad 8 \mid \mathrm{ord}_p(2) \mid p-1 \quad \Rightarrow \quad p \equiv 1 \ (8)$$

E ora per induzione: $\quad K = 2^r \cdot K_r$

$$2^r K_r + 1 \quad \Big| \quad 2^{2^r K_r} + 1$$

Voglio dim che K_r è pari $\Leftrightarrow$ $2^r K_r + 1 \equiv 1$ mod 2^{r+1}. Basta vedere che tutti i divisori primi di $2^{2^r K_r} + 1$ sono $\equiv 1$ mod 2^{r+1}.

$$2^{2^r K_r} \equiv -1 \ (p) \quad \& \quad 2^{2^{r+1} K_r} \equiv 1 \ (p)$$

$\Rightarrow \quad \mathrm{ord}_p(2) \equiv 0$ mod 2^{r+1}, fine.